



欢 迎

AKAE-嵌入式Linux系统工程师培训课程

—— 函数的栈帧

郭同彬

guotongbin@akaedu.org

本次课程内容

★ 函数栈帧

- ☆ 栈
- ☆ 相关汇编指令
- ☆ 实例分析

函数栈帧

★ 栈

- ☆ 满栈、空栈
- ☆ 递增、递减
- ☆ 满递减栈

函数栈帧

★ %eip

☆ == pc 程序计数器，下一条指令地址

★ %ebp

☆ 栈底寄存器

☆ 栈底指针

★ %esp

☆ 栈顶寄存器

☆ 栈顶指针

函数栈帧

★ `push %eax`

☆ `%esp --`

☆ `%eax → (%esp)`

★ `pop %eax`

☆ `(%esp) → %eax`

☆ `%esp ++`

函数栈帧

★ `call addr`

☆ `push %eip` (`call`的下一条指令的地址)

☆ `move addr, %eip`

★ `ret`

☆ `== ~ call`

☆ `pop %eip`

函数栈帧

★ leave

☆ move %ebp, %esp

☆ pop %ebp

函数栈帧实例

```
int main(void)
{
    foo(2, 3);
    return 0;
}
```


函数栈帧实例

```
int foo (int a, int b)
{
    return goo(a, b);
}
```

函数栈帧实例

```
int goo(int c, int d)
{
    int e = c + d;
    return e;
}
```

小结

★ 函数栈帧

结 束

欢迎你到亚嵌来学习！